Инвазивное обследование: кто такие пентестеры

Любая информационная система может содержать уязвимости. Особенно это касается крупных систем, в создании и доработке которых участвовало множество команд. Все ли части системы правильно и до конца настроены? Не осталось ли незакрытых рабочих учетных записей? Не было ли технологического упущения еще на этапе проектирования? На все эти вопросы поможет найти ответы пентест (от англ. Penetration test, pentest — тест на проникновение)!

Цифры говорят сами за себя

~50% веб-приложений содержат уязвимости.

~129 дней уходит на исправление критической уязвимости.

56% — доля систем с тривиальной сложностью преодоления сетевого периметра.

36% — доля успешных атак с получением доступа к конфиденциальным данным.

По данным Application Security Statistics Report 2017 и Positive Technologies за 2016-2018 гг.

Как работает пентестер

Пентестер, используя стандартные и нестандартные инструменты, проверяет системы, которые будут в первую очередь подвергаться атакам, находит уязвимости и смотрит, какие возможности они открывают перед злоумышленниками. Эта работа похожа на действия хакеров, однако пентестеры не доводят дело до деструктивного воздействия. Вместо этого они обращают внимание заказчика на потенциальные «дыры» и помогают их закрыть. Компании и организации, которые всерьез опасаются потери данных или иного ущерба, понимают, что такая проверка поможет им лучше защитить свои системы.

Пентестеров было бы неправильно называть легальными или «белыми» хакерами, скорее, они талантливые программисты и инженеры, профессионалы, которые отлично знают свои инструменты, с помощью которых проверяют системы на прочность.

В компаниях Softline и Infosecurity накоплена обширная экспертиза по пентестированию. Нам хорошо знакомы как стандартные инструменты и регламенты проверки на уязвимость, так и собственные приемы наработки, своеобразные ноу-хау.

Какие виды угроз часто находят пентестеры:

- Несвоевременное обновление ПО.
- Уязвимые веб-приложения. например, для SQL-инъекций.
- Незакрытые рабочие логины.
- Порты в открытом доступе.

Только в 5% случаев пентестер не находит ни одной уязвимости.

Виды тестирования

Разные предметные области охватывают разные виды тестирования. Прежде всего, следует сказать о методах белого, серого и черного ящиков (*рисунок 1*).

Чаще всего заказчики просят протестировать их именно методом черного ящика, так как он наиболее приближен к реальной ситуации.

Зачем заказчику пентест?

Часто мотивом, чтобы обратиться за тестированием на проникновение, становятся для заказчика требования регуляторов. Для организаций, которым требуется независимое подтверждение защищенности, пентест становится доказательством благонадежности перед проверяющими органами. Второй мотив — инциденты ИБ в прошлом. Третий — необходимость защищенного удаленного доступа сотрудников для удаленной работы.

А в отраслях, где от безопасности зависит жизнеспособность бизнеса, регулярное тестирование перед аудитом становится стандартом качества ИБ, своеобразным требованием «цифровой гигиены».

Рисунок 1.

Области проведения пентеста

Внешний пентест и тестирование веб-приложений (Black, Gray box)

Это самый распространенный вид пентестов. Мы обследуем пул IP- или веб-адресов, используемых серверами компании, сканируем их и испытываем на прочность, исходя из знаний технологий атак.

- Поиск в Интернете сайтов заказчика и поддоменов.
- Сканирование портов и определение служб, использующих их.
- Идентификация используемого ПО и технологий.
- Поиск и анализ уязвимостей приложения, входящих в классификацию OWASP.
- Проведение атак, направленных на эксплуатацию уязвимостей (по согласованию с заказчиком).
- Анализ результатов и подготовка рекомендаций.

Внутренний пентест информационных систем (Black, Gray box)

Второй по распространенности вид пентестирования. Пытаемся воспроизвести атаку во внутреннем контуре заказчика.

- Подключение к пользовательскому сегменту сети.
- Анализ трафика протоколов канального и сетевого уровней.
- Физическое внедрение и инструментальное сканирование ресурсов внутренней сети.
- Поиск уязвимостей на обнаруженных ресурсах.
- Проведение сетевых атак и атак, эксплуатирующих уязвимости.
- Получение локальных и доменных учетных записей.
- Анализ результатов и подготовка рекомендаций.

Пентест точек доступа Wi-Fi (Black box)

Осуществляем внешнюю атаку через Wi-Fi:

- Изучение характеристики и особенностей сетей Wi-Fi на объекте.
- Проведение атак на аутентификацию и авторизацию в беспроводных сетях.
- Получение ключей шифрования между клиентом и точкой доступа.
- Проведение атак на аппаратное обеспечение сетей Wi-Fi.
- Установка поддельной точки доступа Wi-Fi, проведение атак на клиентов сетей.
- Обработка результатов и подготовка рекомендаций.

Социотехнический пентест (Black, Gray box)

Симулируем внешнюю атаку с использованием техник социальной инженерии:

- Сбор данных об объекте и пользователях.
- Подготовка провоцирующих данных.
- Рассылка сообщений по электронной почте, через мессенджеры.
- Личные звонки (телефон, Skype).
- Общение через социальные сети.
- Распространение носителей информации с провоцирующими данными.
- Анализ результатов и проведение обучения.
- Взлом паролей на сервисах личного использования и их подбор на корпоративных ресурсах.

Аудит сети (White box)

- Инвентаризация сети.
- Проверка актуальности версий ПО, ошибок конфигурации хостов и межсетевых экранов.
- Поиск и анализ уязвимостей сетевых служб.
- Проверка соответствия межсетевых экранов стандартам ИБ (PCI DSS, NIST, NERC и др.).
- Определение модели атакующего, размещение его в интересующем сегменте сети.
- Проведение сетевых атак (Spoofing, MiTM).
- Построение векторов атак и подготовка плана для минимизации рисков ИБ.

Наши специалисты

Специалисты Infosecurity и Softline постоянно повышают свою квалификацию. В Infosecurity работает 4 сотрудника с редким профессиональным сертификатом OSCP.

OSCP — курс, разработанный компанией Offensive Security, один из немногих общепризнанных профессиональных сертификатов по проведению тестов на проникновение. Это редкий и сложный сертификат, который проходят немногие специалисты. Экзамен длится сутки, дается 6 стендовых машин, к 5 из которых надо получить полный доступ. Вторые сутки даются претенденту на написание отчета. Специалистов по пентестингу со статусом OSCP в России совсем немного, а в Infosecurity уже 4 человека сдали этот экзамен.

Отчетность

Результатом пентеста становится отчет с рекомендациями по модернизации приложений, сетей, настроек серверов для закрытия существующих «дыр» в безопасности.

Пример реализации

КОМПАНИЯ «А»: 5000 сотрудников, 6 филиалов, 160 B2B-клиентов (крупных и средних интернет-магазинов).

РЕЗУЛЬТАТЫ: Выявлено 12 уязвимостей с низким уровнем риска, 5 — со средним, 2 — с высоким. Самая критичная уязвимость — SQL-инъекция на веб-портале, которая позволяет злоумышленнику получить контроль над сервером баз данных. Даны рекомендации, как повысить защищенность системы с учетом всех выявленных уязвимостей.

МЕРОПРИЯТИЯ: Внешний пентест, включая тестирование веб-приложений методом «черного ящика»

СРОКИ: 25 рабочих дней

НАШИ ПРЕИМУЩЕСТВА

- Сертифицированные сотрудники (Pentestit, OSCP).
- Гибкий подход: от обследования отдельных компонентов (Wi-Fi, сайт и т.д.) до комплексного обследования.
- Опыт работы с разными компаниями: финансовыми, государственными, промышленными.
- Использование собственных ноу-хау, высокотехнологичного аппаратного обеспечения и методологий.